DIGITAL RIGHTS MANAGEMENT TERAPAN SERTA ANCAMANNYA

Aloysius Adrian – NIM : 13506031

Program Studi Teknik Informatika, Institut Teknologi Bandung
Jl. Ganesha 10, Bandung
E-mail : if16031@students.if.itb.ac.id

Abstrak

Berbagai isu pembajakan pada karya sudah dianggap hal yang klise. Pembajakan dianggap sudah terlalu lazim ditemukan sehingga masyarakat seolah tidak lagi peduli. Dari dulu, telah banyak upaya dilakukan untuk menghambat pembajakan. Salah satu teknik yang ampuh adalah dengan menerapkan *Digital Rights Management*, disingkat DRM, pada berkas audio atau video yang baru saja marak. Penerapan DRM pada berkas audio telah cukup lama beredar. Dengan penerapan DRM pada berkas audio, hak akses untuk memutar lagu terbatas pada orang yang memiliki hak saja. Maksudnya, bila seseorang membeli berkas audio dengan DRM terintegrasi di dalamnya, berkas audio itu hanya dapat dimainkan pada komputer orang tersebut. Bila berkas audio disebarkan lagi pada rekannya, berkas audio tidak dapat dimainkan.
Sebuah teknik yang cukup ampuh diterapkan untuk mengurangi dan menghambat peredaran berkas audio secara ilegal, namun tentu saja teknik ini memiliki banyak jenis ancaman untuk mampu menembus pengamanan DRM pada berkas audio ini seperti konversi audio, reverse-engineering, dan juga beberapa teknik lain.

***Kata kunci**: enkripsi, dekripsi, fairplay, DRM*

1. Pendahuluan

Sebuah berkas audio atau video tentu saja diinginkan pengguna atau penikmat untuk mempu dimainkan di mana saja dan kapan saja. Umumnya, sebuah berkas audio atau video mampu dimainkan di mana saja dan kapan saja asalkan perangkat pemutarnya mendukung. Misalkan saja dalam sebuah unit komputer, atau pemutar cakram, dan lain - lain. Sekarang ini, seseorang sering terlihat bekerja sambil mendengarkan musik dari komputer atau laptopnya, atau mendengarkan dari pemutar musik digital. Ketika berjalan - jalan, atau bahkan ketika berkendara (yang ini tidak dianjurkan karena mampu membahayakan). Saat ini, begitu banyak situs penyedia berkas audio untuk diunduh secara ilegal alias bajakan. Hal ini tentu saja sangat merugikan. Moral masyarakat seperti telah terbungkam dan selalu mencari yang gratis dengan mengunduh versi bajakan tanpa memerhatikan hak cipta atau kerja keras usaha penggubah lagu. Tentu saja telah banyak upaya untuk mengurangi atau bahkan menghilangkan secara total budaya bajakan ini. Salah satu teknik yang cukup ampuh adalah dengan memberi pengaman pada berkas multimedia. Ketika berbagai upaya mencegah pembajakan ini dilakukan dan dirasa kurang berpengaruh, teknik pengaman pada berkas multimedia digital ini dipercaya mampu menekan angka pembajakan secara signifikan. Teknik pemberian pengaman pada berkas multimedia, seringnya berkas audio diberi nama DRM. Digital Rights Management.
Secara sederhana, DRM adalah teknik untuk mengendalikan akses informasi. Seorang pengguna, penikmat musik ingin mendapat akses untuk menikmati berkas audio sedangkan perusahaan musik ingin melindungi hak intelektual mereka dari penggunaan ilegal. DRM meyediakan solusi untuk kedua pihak.

Pembatasan oleh DRM adalah dengan membatasi berkas audio untuk hanya dapat dimainkan pada pemutar tertentu. Namun dewasa ini sudah berkembang sehingga pembatasan dapat lebih fleksibel. Berkas audio yang diproteksi dengan DRM dapat dibakar pada cakram, bahkan dapat dibatasi hingga 10 kali dibakar dalam cakram sebelum akhirnya tidak dapat lagi.

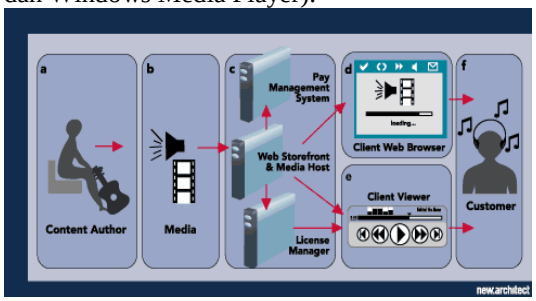
Ada banyak teknik DRM lainnya, antara lain DRM sistem yang hanya dapat berjalan di lingkungan Windows saja. Ada juga sistem DRM yang mampu memberikan "ganjaran" bagi pengguna yang hendak menyalahgunakan media DRM. Beberapa media mampu secara programatis mematikan komputer bila ternyata komputer tersebut tidak memiliki hak akses legal terhadap DRM. Bahkan sebuah album kumpulan musik Celine Dion tahun 2002 yang diproduksi oleh EPIC dan Sony Records mampu merusakkan komputer bila cakramnya dimasukkan ke dalam CD-ROM.

2. Penjelasan Digital Rights Management

Pengaplikasian DRM pada berkas multimedia melingkupi pokok - pokok berikut ini.

- Data protection, sehingga berkas tidak dapat diakses tanpa diberi akses khusus.
- Identifikasi yang unik untuk setiap kostumer untuk menjamin hak akses khusus diterapkan secara tepat.
- Manajemen hak secara terpusat untuk mencegah pembobolan, atau untuk mendistribusikan berkas dengan gratis.
- Fleksibilitas, agar sistem DRM dapat diterapkan pada berbagai bidang.

DRM memiliki kelebihan dan kekurangan sendiri dibandingkan dengan metode pengamanan sebelumnya (watermark atau password). Kelebihannya adalah DRM lebih fleksibel dan lebih mudah untuk diubah hak aksesnya. Penyedia atau pemberi hak akses pada server terpusat dapat dengan cepat mengatur hak akses media. Kekurangannya adalah dengan perlunya pengaturan hak akses (autorisasi atau pemberian hak akses baru) di server terpusat, maka terntu saja dibutuhkan koneksi internet. Selain itu, tentu saja pemutar berkas multimedia tersebut juga haruslah pemutar khusus yang memang diprogram untuk mampu mengautentikasi berkas DRM (contohnya iTunes dan Windows Media Player).



Gambar 1 Anatomi DRM

Anatomi DRM : secara sederhana, proses DRM dimulai dari (a) penyedia konten atau berkas yang menyiapkan (b) berkas multimedia berupa audio atau video atau lainnya dalam rupa berkas digital tentunya. Berkas tersebut lalu dienkripsi untuk mencegah dari pelanggaran hak akses dan disimpan pada (c) server yang juga berfungsi untuk mengatur hak akses. Berkas lalu akan didekripsi ketika sampai di pihak pengguna melalui (d) browser atau (e) pemutar berkas yang mendukung. Lalu (e) pengguna yang memiliki hak akses secara sah akan dapat menikmati berkas tersebut.

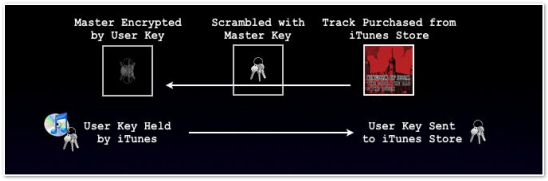
Sistem DRM menganut dua pendekatan untuk mengamankan isi dari berkas multimedia. Pertama adalah "containment", konten dienkripsi sehingga hanya dapat diakses oleh pengguna yang terautorisasi. Kedua adalah "marking", memberikan watermark pada berkas atau flag, atau tag XrML pada konten sebagai penanda bagi alat pemutar berkas bahwa berkas tersebut diproteksi.

Ada dua teknik pengaman DRM pada berkas audio yang terkenal. Masing - masing dicetuskan dan digunakan oleh dua perusahaan raksasa yang sejak dahulu menjadi rival, Apple Company dan Microsoft Corporation. Apple memperkenalkan sistem DRM Fairplay.

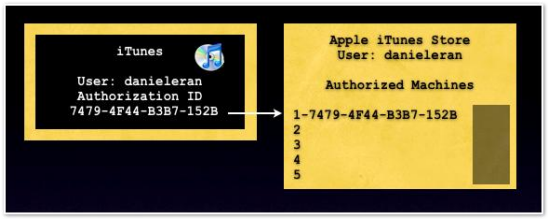
2.1 Apple Fairplay DRM

Fairplay adalah teknologi DRM yang berbasis pada teknologi ciptaan perusahaan bernama Veridisc. Fairplay dimasukkan ke dalam media berjenis QuickTime dan dapat digunakan dalam iPhone, iPod, dan iTunes yang notabenenya merupakan pemutar digital keluaran Apple. Fairplay secara digital mengenkripsi berkas audio dengan format AAC dan mencegah penggunaan ilegal. Berkas multimedia yang terenkripsi oleh Fairplay pada dasarnya merupakan berkas MP4 biasa yang audio streamnya terenkripsi dengan AAC. Audio stream ini terenkripsi dengan algoritma AES yang dikombinasikan dengan hash MD5. Diperlukan sebuah kunci utama untuk mendekripsi berkas ini, dan kunci utama ini juga tersimpan dalam bentuk terenkripsi dalam berkas MP4 yang utama. Kunci yang diperlukan untuk mendekripsi kunci utama ini yang disebut kunci pengguna (user key). Setiap kali pengguna membeli atau mengunduh berkas audio dari toko musik online milik Apple (iTunes Store), sebuah

kunci random baru dihasilkan dan digunakan untuk mengenkripsi kunci utama. Kunci random ini disimpan bersamaan dengan informasi akun pengguna (pembeli) pada server Apple dan dimasukkan juga ke dalam pemutar musik iTunes pada komputer pengguna.



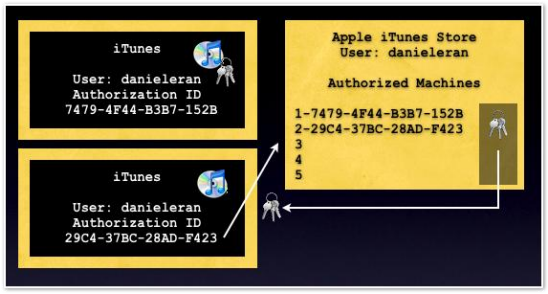
Gambar 2 Teknik Pemberian DRM



Gambar 3 Kunci terpasang pada pemutar media iTunes

Pada pemutar iTunes terdapat sebuah penyimpanan kunci - kunci pengguna untuk mendekripsi kunci utama pada masing - masing berkas audio. Dengan kunci ini, pengguna dapat dengan leluasa memutar lagu pada komputer yang telah terautentikasi. DRM Fairplay tidak memegaruhi kualitas suara. Fairplay juga tidak bisa melindungi berkas untuk dibakar pada cakram. Fairplay hanya berfungsi melindungi konten audio pada berkas multimedia.
Batasan dari DRM Fairplay antara lain adalah

- Berkas dapat dikopi pada pemutar music iPod yang terbatas.
- Berkas dapat dimainkan pada maksimal 5 komputer yang telah diberi autorisasi.



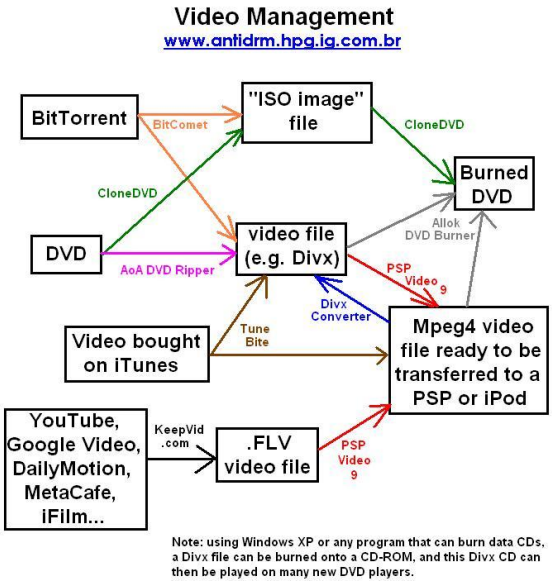
Gambar 4 Mencocokkan kunci pada pemutar iTunes di komputer berbeda

2.2 Windows Media DRM

Microsoft dengan sistem DRM Windows Media (WMDRM). WMDRM fungsinya sama dengan DRM Fairplay, dan fungsi DRM secara umum yakni membatasi hak akses sebuah berkas multimedia. Sama seperti Fairplay, berkas dengan WMDRM hanya dapat dimainkan dalam lingkunan Microsoft Windows saja.
Cara kerja WMDRM adalah perangkat lunak sisi pengguna akan menerima plain teks K sepanjang 7 byte yang berisi kunci dari lisensi di server. Server mengenkripsi kunci sebelum mengirimkannya pada pengguna dengan kunci ECC sepanjang 160 bit. Server juga mengirimkan ID kunci konten tanpa dienkripsi. Pada sisi pengguna lalu kunci K sebagai kunci RC4 untuk mendekripsi berkas yang terenkrip WMDRM. Berkas multimedia yang terlindungi WMDRM memiliki format WMA (Windows Media Audio). Berkas WMA ternyata mampu memperbarui perlindungannya. Microsoft telah berasumsi bahwa kemungkinan WMDRM terpatahkan sangat besar, maka Microsoft menyiapkan sebuah cara untuk dapat memperbarui perlindungan secara online.

3. Ancaman DRM

Walaupun terdengar hebat, perlindungan DRM tetap dapat dipatahkan. Berbagai perangkat lunak dikembangkan oleh pihak yang menolak DRM, programmer - programmer handal untuk menghilangkan tag atau tanda DRM dalam berkas audio yang terproteksi. Pada dasarnya, perangkat lunak ini tidak mengubah konten musiknya, namun menghilangkan proteksi dari konten pada berkas audio sehingga berkas audio tetap dapat diputar tanpa mengubah musiknya. Salah satu cara yang cukup merepotkan namun ampuh untuk mematahkan proteksi DRM adalah dengan mambakar berkas audio ke dalam cakram. Dengan dibakar pada cakram, dapat dipastikan bahwa proteksi DRM tidak ikut tercantumkan. Setelah terbakar dalam cakram, berkas audio dapat dikopi kembali menjadi berkas lunak audio yang bebas proteksi DRM. Lebih banyak lagi berkas multimedia terproteksi DRM yang dapat dipatahkan dengan cara yang mirip dengan di atas. Gambar berikut dapat menggambarkan nama perangkat lunak yang mampu menghilangkan DRM serta alur - alur pengubahannya.



Gambar 5 Alur pemecahan DRM pada berkas multimedia

Untuk berkas yang diberi proteksi DRM secara online melalui server terpusat, contohnya DRM Fairplay, ada teknik cerdik yang sedikit rumit untuk mampu mematahkan pengamanan DRM yakni dengan menulis program sederhana yang mampu mengekstrak informasi mengenai kunci K di sisi pengguna dan memanfaatkannya untuk berpura - pura meminta kunci untuk mendekripsi kunci iTunes.
Ada juga teknik yang menyamarkan pemutar media iTunes atau Windows Media Player dan berpura - pura mengunduh berkas audio dari server namun tidak disertai pengamanan (penguncian) DRM. Karena server pusat mengira tipe pemutar adalah pemutar yang sah, maka tidak akan terjadi masalah pengaksesan server.

Teknik pemecahan DRM Fairplay yang saya sarankan.
Menurut saya, ada satu teknik yang pernah saya coba sendiri untuk menghilangkan DRM dari Fairplay Apple adalah dengan memutar berkas audio pada komputer yang secara sah memiliki akses, dan secara bersamaan kembali merekamnya ke dalam sebuah berkas audio sementara lainnya. Setelah proses selesai, saya mampu mengambil berkas salinan ini untuk kemudian dikompresi lagi dengan kompresi MP3 atau sebagainya.

4. Kesimpulan

Terapan DRM di tahun 200 ternyata mengalami perubahan drastis. Pihak Apple Company memutuskan untuk tidak lagi melindungi seluruh lagu yang dijualnya dengan DRM. Alasannya, memang sejak awal, penerapan DRM ini mengundang pro-kontra. Banyak orang yang menentang penerapan DRM ini karena dianggap tidak seusai konteks. Di mana pada dasarnya tujuan DRM adalah melindungi hak kepemilikan, namun justru membatasi pemilik untuk memakai benda yang telah dibelinya. Bayangkan saja bila kita membeli sebuah sepeda. Kita tentu saja bebas untuk melakukan apa saja pada sepeda kita, entah dicat ulang atau diganti rantainya, dan lain – lain. Sama halnya dengan berkas digital. Anggap saja kita telah membeli sebuah DVD secara legal. Tentu saja kita ingin memanfaatkan konten DVD yang telah kita beli secara legal dengan semaksimal mungkin. Namun nyatanya, DRM sangat membatasi perilaku penggunanya terhadap benda yang telah dibeli haknya.

Sejak utama, Apple berpendapat bahwa untuk melindungi lagu yang dibeli atas lisensi Apple hanya dapat dimainkan dalam lingkungan produk Apple saja, maka DRM perlu diterapkan, namun justru ini menjadi bumerang yang menjadikan pengguna enggan untuk membeli melalui iTunes Store dan berpindah untuk mengunduh berkas audio dari tempat lain secara legal dan lebih mudah. Selain itu, penjualan lagu dengan DRM ternyata kalah dengan penjualan lagu tanpa DRM. Untuk menekan kerugian, maka Apple memutuskan untuk tidak lagi melindungi dengan DRM. Dan begitu pula dengan Microsoft yang juga menghilangkan pengamanan WMDRM.

5. Daftar Pustaka

[1] Munir, Rinaldi. *Diktat Kuliah IF5054 Kriptografi.* Penerbit ITB 2006

[2] http://www.eff.org/wp/digital-rights-management-failure-developed-world-danger-developing-world/ - Tanggal akses 15 Mei 2009

[3] http://www.eff.org/issues/drm - Tanggal akses 15 Mei 2009

[4] http://www.roughlydrafted.com/drm - tanggal akses 15 Mei 2009